Attorney Docket No. 9564-17 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application: Stefan Andersson
Application No.: 10/589,171
Filed: August 11, 2006
For: METHOD AND APPARATUS FOR PROVIDING DYNAMIC SECURITY MANAGEMENT

Confirmation No.: 6861
Group Art Unit: 2431
Examiner: Longbit Chai

Date : January 4, 2010

Mail Stop Appeal Brief -Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith is the APPEAL BRIEF for the above-identified application, pursuant to the Notice of Appeal filed on November 2, 2009.

2. This application is filed on behalf of
☐ a small entity.

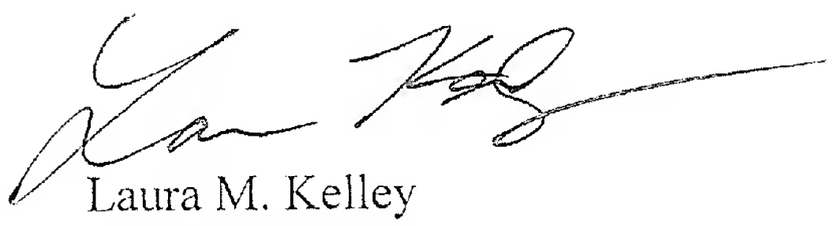
3. Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:
☐ small entity $270.00
☒ other than small entity $540.00

Appeal Brief fee due $540.00

☐ Please first reapply any previously paid notice of appeal fee and appeal brief.

☒ Any additional fee or refund may be charged to Deposit Account 50-0220.

Respectfully submitted,



Laura M. Kelley
Registration No. 48,441

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 54414

Attorney Docket No. 9564-17 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application: Stefan Andersson
Application No.: 10/589,171
Filed: August 11, 2006
For: METHOD AND APPARATUS FOR PROVIDING DYNAMIC SECURITY MANAGEMENT

Confirmation No.: 6861
Group Art Unit: 2431
Examiner: Longbit Chai

Date : January 4, 2010

Mail Stop Appeal Brief -Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.67

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed November 2, 2009.

Real Party In Interest

The real party in interest is assignee Sony Ericsson Mobile Communications AB by virtue of an Assignment recorded at Reel No. 021690 and Frame No. 0784.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Claims 1-35 are pending and stand rejected. Appellants appeal the final rejection of Claims 1-35 by the Final Office Action dated July 2, 2009 (the Action). The Action rejects Claims 1-3 and 9-20 under 35 U.S.C. 102(a) as being anticipated by EP 1361527 to Anderson (Anderson). Claims 4-8 and 21-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson in view of U.S. Patent No. 6,760,912 to Yarsa (Yarsa).

As noted in Appellants' paper dated May 26, 2009, Claims 26-35 are discussed in the Action on pages 4-7 in the 35 U.S.C. 102(a) rejections. However, Claims 26-35 are not identified in the rejection under 35 U.S.C. 102(a) on page 3 of the Action. Appellants will treat Claims 26-35 as also being rejected in the Action under 35 U.S.C. 102(a) as discussed on pages 4-7 of the Action for purposes of this Appeal Brief. Claims 26-35 are excluded from the headings in the Argument section below for consistency with the Action.

Status of Amendments

The Appendix of Claims submitted herewith reflects the state of the claims of record.

Summary of Claimed Subject Matter

Claim 1 recites a method of providing a dynamic security management in an apparatus. *See*, *e.g.*, page 5, lines 11-14. The apparatus includes a platform for running an application (*see*, *e.g.*, page 5, lines 30-31); a security manager for handling access of the application to functions existing in the apparatus (*see*, *e.g.*, page 5, lines 29-32; security manager 7, Figure 2); an application interface between the platform and the application (*see*, *e.g.*, page 5, lines 31-32; application interface 11, Figure 2); and a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface (*see*, *e.g.*, page 5, lines 33-35). The method includes downloading into the apparatus an object containing access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus (*see*, *e.g.*, page 5, lines 36-39; page 6, lines 17-29). The permissions are applicable to at least one function, and the object comprising new routines and/or new functions (*see*, *e.g.*, page 6, lines 17-29). The object is verified (*see*, *e.g.*, page 7, line 10), and the access permissions are installed together with the existing permissions (*see*, *e.g.*, page 7, lines 14-15). The object enhances the application interface with the new routines and/or new functions (*see*, *e.g.*, page 2, lines 18-19; page 8, lines 9-12).

Claim 14 recites a method of providing a dynamic security management in an apparatus. *See*, *e.g.*, page 5, lines 11-14. The apparatus includes a platform for running an application (*see*, *e.g.*, page 5, lines 30-31); a security manager for handling access of the

application to functions existing in the apparatus (*see*, *e.g.*, page 5, lines 29-32; security manager 7, Figure 2); an application interface between the platform and the application (*see*, *e.g.*, page 5, lines 31-32; application interface 11, Figure 2); and a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface (*see*, *e.g.*, page 5, lines 33-35). The method includes storing the access permissions in a security policy and downloading into the apparatus an object containing additional access permissions and other permission information to be associated with policy contained in the downloaded object as well as the access permissions in the security policy (*see*, *e.g.*, page 6, lines 17-29). The permissions are applicable to at least one function and the object includes new routines and/or new functions (*see*, *e.g.*, page 6, lines 17-29). The security policy is provided with a hierarchical structure including the access permissions in the security policy and the object containing additional access permissions and other permission information so that the object enhances the application interface with the new routines and/or new functions (*see*, *e.g.*, page 2, lines 18-19; page 8, lines 9-12;page 8, lines 15-23).

Claim 18 recites an apparatus with dynamic security management including a platform for running an application (*see*, *e.g.*, page 5, lines 30-31); a security manager for handling access of the application to functions existing in the apparatus (*see*, *e.g.*, page 5, lines 29-32; security manager 7, Figure 2); an application interface between the platform and the application (*see*, *e.g.*, page 5, lines 31-32; application interface 11, Figure 2); and a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface (*see*, *e.g.*, page 5, lines 33-35). The apparatus is configured to download an object containing access permissions and other permission information to be associated with policy contained in the downloaded objects as well as access permissions already existing in the apparatus (*see*, *e.g.*, page 5, lines 36-39; page 6, lines 17-29). The permissions are applicable to at least one function, and the object comprising new routines and/or new functions (*see*, *e.g.*, page 6, lines 17-29). The object is verified (*see*, *e.g.*, page 7, line 10), and the access permissions are installed together with the existing permissions (*see*, *e.g.*, page 7, lines 14-15). The object enhances the application interface with the new routines and/or new functions (*see*, *e.g.*, page 2, lines 18-19; page 8, lines 9-12).

Claim 31 recites an apparatus for providing a dynamic security management including a platform for running an application (*see*, *e.g.*, page 5, lines 30-31); a security manager for handling access of the application to functions existing in the apparatus (*see*, *e.g.*, page 5, lines 29-32; security manager 7, Figure 2); an application interface between the platform and the application (*see*, *e.g.*, page 5, lines 31-32; application interface 11, Figure 2); and a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface (*see*, *e.g.*, page 5, lines 33-35). The apparatus is configured to store the access permissions in a security policy, and to provide the security policy with a hierarchical structure (*see*, *e.g.*, page 6, lines 17-29). The apparatus is configured to download an object containing additional access permissions to be associated with policy contained in the downloaded objects as well as access permissions already existing in the apparatus (*see*, *e.g.*, page 6, lines 17-29). The permissions are applicable to at least one function, and the object comprising new routines and/or new functions (*see*, *e.g.*, page 6, lines 17-29). The object is verified (*see*, *e.g.*, page 7, line 10), and the access permissions are installed together with the existing permissions (*see*, *e.g.*, page 7, lines 14-15). The object enhances the application interface with the new routines and/or new functions (*see*, *e.g.*, page 2, lines 18-19; page 8, lines 9-12).

Grounds of Rejection to be Reviewed on Appeal

1. Whether Claims 1-3, 9-20 and 26-35 are properly rejected under 35 U.S.C. 102(a) as being anticipated by Anderson.

2. Whether Claims 4-8 and 21-25 are properly rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson in view of Yarsa.

Argument

I. Claims 1-3 and 9-20 are Patentable under 35 U.S.C. 102(a) over Anderson

Claim 1 recites as follows:

> A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application; a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and

used by the security manager for controlling access of the applicationto functions through the application interface the method comprising:

downloading into the apparatus an object containing access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions;

verifying the object; and

installing the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

Anderson proposes a method for loading an application in a device. In order to operate in the device, the application in Anderson apparently accesses functions of the device. The application's access to functions of the device is controlled through an interface unit API governed by access rights. In Anderson, the access rights are defined by preloaded attribute certificates. The access rights control what functions may be accessed by the application. *See* Anderson, paragraphs [0020]-[0021]. The Action apparently takes the position that the attribute certificates are analogous to the access permissions and the object recited in Claim 1.

Appellants submit that the access rights that are defined by *preloaded* attribute certificates in Anderson do not disclose or render obvious the recitations of Claim 1. For example, Anderson does not disclose that a downloaded *object* includes *access permissions* and other permission information to be associated with policy contained *in the downloaded object* as well as access permissions already existing in the apparatus. Moreover, Anderson does not disclose that the access permissions are installed together with the existing permissions or that the object enhances the application interface with new routines and/or new functions.

In Anderson, the attribute certificate is generic, *i.e.*, the attribute certificate is valid for several different applications and is used in order to give applications correct access rights. *See* Anderson, paragraph [0024]. Appellants cannot locate any portion of Anderson that discusses any new routines and/or new functions that are provided by the attribute certificate. Therefore, the attribute certificates of Anderson cannot be considered analogous to the object

recited in Claim 1, which enhances the application interface with new routines and/or new functions.

The Action states that Anderson discloses that the user can download the new functions or applications such as tools to upgrade the user **device**. *See* the Action, page 3. However, the tools in Anderson do not teach enhancing the **application interface** as recited in Claim 1. Appellants submit that prior art devices, such as Anderson, which run in a Java environment (*see* Anderson, paragraph [0019]), do not provide the addition of a library that provides the Java environment access through Java application programming interface (API) to various functions (for example, a calendar database or the like). In Anderson, a security manager checks the access permissions of a MIDIlet against a security policy predefined in the phone and controls the API. According to Anderson, the security manager is apparently static, and it does not appear to be possible to add API functionality. *See* Anderson, paragraphs [0021]-[0024].

Accordingly, Anderson relates to generic attribute certificates, which are used to limit the access to an API for a number of applications provided by, *e.g.*, a third party software supplier. In contrast, the current claims relate to changing the current security policy in a security manager, and recite:

> downloading into the apparatus an object containing access permissions and other permissions to be associated with a policy contained in the downloaded object as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new function.

Accordingly, the access permissions of Claim 1 are therefore not analogous to the attribute certificate discussed in Anderson.

Moreover, Anderson states as follows:

> The attribute certificate contains at least information about the issuer, subject validity (optional) and a signature and for the purpose of the present invention information about access rights. In other words, the attribute certificate defines a **generic** profile for controlling the interface 4 in connection with one or several applications to be associated with the profile.

See Anderson, paragraph [0024] (cited in the Action)(emphasis added).

Appellants respectfully disagree with the Action's characterization that this portion of Anderson, which does not mention anything about access permissions associated with a downloaded object or including new routines. However, paragraph [0024] of Anderson clearly states that the attribute certificate contains a generic profile to be used in connection with several applications. Thus, Anderson proposes an attribute (or authority) certificate, but does not propose downloading an object containing access permissions and other permissions to be associated with a policy contained in the downloaded object as well as access permissions already existing in the apparatus such that the permissions are applicable to at least one function or that the object includes new routines and/or new functions.

In addition, the Action refers to column 2, lines 50-52 (paragraph [0016]) of Anderson as allegedly disclosing that the attribute certificate is downloaded together with the application. *See* the Action, page 2. However, Anderson never states that the downloading is performed together as recited in Claim 1. In contrast, Anderson relates to pre-loaded generic attribute certificates that are not downloaded together with the application. Moreover, the pre-loaded generic attribute certificates of Anderson clearly do not include an object enhancing the application interface with new routines and/or new functions. In fact, the generic attribute certificates of Anderson appear to be used by several functions such that they are not downloaded together with the application.

The access permissions according to the present invention are installed with existing security permissions, *i.e.*, Claim 1 recites "installing the access permissions together with the existing permissions," when downloading the object, which contains new routines and/or new functions and permissions applicable thereto. Accordingly, when the access permissions are downloaded, the existing policy is extended or changed in accordance with the new access permissions, and a dynamic security management is achieved. In contrast, the attribute certificate in Anderson is used when installing an application such that the existing attribute certificate is then controlling the interface via the security manager, and the security manager holds the security policy. Thus, Anderson cannot provide dynamic enhancement of the user interface.

Accordingly, the access rights that are defined by *preloaded* attribute certificates in Anderson do not disclose or render obvious the recitations of Claim 1, *i.e.*, that the downloaded *object* includes *access permissions* and other permission information to be

associated with policy contained *in the downloaded object* as well as access permissions already existing in the apparatus.

Accordingly, Appellants submit that the recitations of Claim 1 are not disclosed or rendered obvious by the cited prior art. Independent Claims 14, 18 and 31 include recitations similar to Claim 1 and are likewise patentable over the cited art for at least the reasons discussed above. Claims 2-3, 9-17, 19, 26-30 and 32-35 depend from the independent claims discussed above. Accordingly, Appellants request that the rejection of Claims 1-3, 9-20 and 26-35 be reversed.

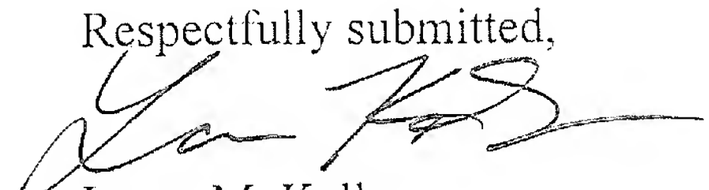
II. Claims 4-8 and 21-25 are patentable under 35 U.S.C. 103(a) over Anderson in view of Yarsa

Claims 4-8 depend from Claim 1, and Claims 21-25 depend from Claim 18. Thus, Claims 4-8 and 21-25 are patentable at least per the patentability of Claims 1 and 18 discussed above. It is further noted that Yarsa does not provide the missing elements of Anderson discussed above. Accordingly, Appellants request that the rejection of Claims 4-8 and 21-25 be reversed.

CONCLUSION

In view of the above discussion, Appellants submit that the rejection of Claims 1-22 should be reversed and the present application passed to issue.

Respectfully submitted,

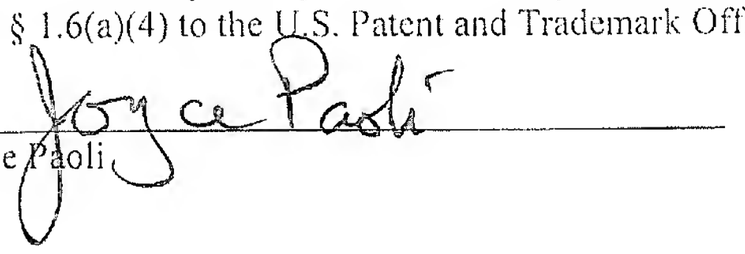


Laura M. Kelley
Attorney for Appellants
Registration No. 48,441

Customer No. 54414
Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on January 4, 2010.



Joyce Paoli

Claims Appendix

1. (Previously Presented) A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application; a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface the method comprising:

downloading into the apparatus an object containing access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions;

verifying the object; and

installing the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

2. (Previously Presented) A method according to claim 1, wherein the object is verified by checking a certificate chain of the object.

3. (Previously Presented) A method according to claim 1–further comprising verifying that a policy of the function allows updates.

4. (Previously Presented) A method according claim 1, further comprising installing a library comprising new routines and/or new functions to be called by an application or another library stored in the apparatus to enable access of functions through the application interface.

5. (Previously Presented) A method according to claim 4, wherein the new routines and/or new functions can access existing functions through the library.

6. (Previously Presented) A method according to claim 5, wherein the security manger, when accessing functions, recursively checks the permissions of the application interfaces and libraries in a linked chain related to the called functions.

7. (Previously Presented) A method according to claim 1, further comprising installing a new function so that the new function can access existing functions through the application interface.

8. (Previously Presented) A method according to claim 7, wherein the new functions can access existing functions through a library.

9. (Previously Presented) A method according claim 1, wherein the access permissions are contained in a policy file.

10. (Previously Presented) A method according to claim 9, wherein the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

11. (Previously Presented) A method according to claim 9, wherein the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

12. (Previously Presented) A method according to claim 11, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

13. (Previously Presented) A method according to claim 10, wherein the policy file has a structure including logical expressions.

14. (Previously Presented) A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application;

a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface, the method comprising:

storing the access permissions in a security policy;

downloading into the apparatus an object containing additional access permissions and other permission information to be associated with policy contained in the downloaded object as well as the access permissions in the security policy, wherein the permissions are applicable to at least one function and the object includes new routines and/or new functions; and

providing the security policy with a hierarchical structure including the access permissions in the security policy and the object containing additional access permissions and other permission information so that the object enhances the application interface with the new routines and/or new functions.

15. (Previously Presented) A method according to claim 14, wherein the security policy has a structure linking access levels of existing functions with a domain associated with the downloaded object.

16. (Previously Presented) A method according to claim 15, wherein the security policy has a structure linking access levels of existing functions with information contained in a certificate chain.

17. (Previously Presented) A method according to claim 16, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

18. (Previously Presented) An apparatus with dynamic security management comprising:

a platform for running an application;

a security manager for handling access of the application to functions existing in the apparatus;

an application interface between the platform and the application;

a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface wherein the apparatus is configured to download an object containing access permissions and other permission information to be associated with policy contained in the downloaded objects as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions; to verify the object; and to install the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

19. (Previously Presented) An apparatus according to claim 18, wherein the security manager is configured to verify the object by checking a certificate chain of the object.

20. (Previously Presented) An apparatus according to claim 18 wherein the security manager is configured to verify that a policy of the function allows updates.

21. (Previously Presented) An apparatus according to claim 18, wherein the apparatus is configured to install a library comprising new routines and/or new functions to be called by an application or another library stored in the apparatus to enable access of functions through the application interface.

22. (Previously Presented) An apparatus according to claim 21, wherein the new routines and/or new functions can access existing functions through the library.

23. (Previously Presented) An apparatus according to claim 22, wherein the security manger, when accessing functions, is configured to recursively check the

permissions of the application interfaces and libraries in a linked chain related to the called functions.

24. (Previously Presented) An apparatus according claim 18, wherein the apparatus is configured to install a new function so that the new function can access existing functions through the application interface.

25. (Previously Presented) An apparatus according to claim 24, wherein the new functions can access existing functions through a library.

26. (Previously Presented) An apparatus according to claim 18, wherein the access permissions are contained in a policy file.

27. (Previously Presented) An apparatus according to claim 26, Previously Presented wherein the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

28. (Previously Presented) An apparatus according to claim 26, wherein the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

29. (Previously Presented) An apparatus according to claim 28, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

30. (Previously Presented) An apparatus according to claim 28, wherein the policy file has a structure including logical expressions.

31. (Previously Presented) An apparatus for providing a dynamic security management comprising:

a platform for running an application;

a security manager for handling access of the application to functions existing in the apparatus;

an application interface between the platform and the application;

a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface, wherein the apparatus is configured to store the access permissions in a security policy; and provide the security policy with a hierarchical structure, wherein the apparatus is configured to download an object containing additional access permissions to be associated with policy contained in the downloaded objects as well as access permissions already existing in teh apparatus, wherein the permissions are applicable to at least one function, said object comprising new routines and/or new functions; to verify the object; and to install the access permissions together with the existing permissions; said object enhancing the application interface with the new routines and/or new functions.

32. (Previously Presented) An apparatus according to claim 31, wherein the security policy has a structure linking access levels of existing functions with a domain associated with the downloaded object.

33. (Previously Presented) An apparatus according to claim 32, wherein the security policy has a structure linking access levels of existing functions with information contained in a certificate chain.

34. (Previously Presented) An apparatus according to claim 33, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

35. (Previously Presented) An apparatus according to claim 18, wherein the apparatus is a portable telephone, a pager, a communicator, a smart phone, or an electronic organiser.

Evidence Appendix

NONE

Related Proceedings Appendix

NONE